Playing the Identity Card

Playing the Identity Card

Surveillance, security and identification in global perspective

Edited by Colin J. Bennett and David Lyon

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2008
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

Simultaneously published in the USA and Canada
by Routledge
270 Madison Ave, New York, NY 10016

Routledge is an imprint of the Taylor & Francis Group,
an informa business

Typeset in Times New Roman
by Swales and Willis Ltd, Exeter, Devon
Printed and bound in Great Britain by Antony Rowe Ltd, Chippenham,
Wiltshire

British Library Cataloguing in Publication Data
A catalogue record for this book is available
from the British Library

Library of Congress Cataloging in Publication Data
A catalog record has been requested for this book

ISBN

Contents

Contributors

Louise Amoore specializes in the geopolitics of risk and security in the Department of Geography, Durham University, UK. She is currently leading two Economic and Social Research Council (ESRC) projects on risk and the technologies of the War on Terror: 'Contested Borders' and 'Data Wars'. She is co-editor (with Marieke deGoede) of *Risk and the War on Terror* (London: Routledge, 2008), and has published some of her recent work in *Security Dialogue*, *Political Geography*, *Antipode* and *Transactions*.

Colin J. Bennett is a Professor in the Department of Political Science at the University of Victoria, Canada. His research is focused on the comparative analysis of surveillance technologies and privacy protection policies at the domestic and international levels. He has published three books on the topic: *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, 1992); *Visions of Privacy: Policy Choices for the Digital Age* (University of Toronto Press, 1999, with Rebecca Grant); *The Governance of Privacy: Policy Instruments in the Digital Age* (Ashgate Press, 2003; with Charles Raab, MIT Press, 2006).

Krista Boa is a PhD candidate at the Faculty of Information Studies, University of Toronto, Canada. Her research focuses on the development of technology-based identification systems, such as machine-readable travel documents and national ID cards, by examining the ways in which technologies are framed discursively. She is interested in how these discourses influence the design of the system and transform conceptions of identity, anonymity and privacy. Other related areas of interest which inform her research include: surveillance, access to information, and conceptualizations of privacy, particularly legal and theoretical arguments about reasonable expectations of privacy in public.

Keith Breckenridge is an Associate Professor of History and Internet Studies at the University of KwaZulu-Natal, South Africa. His current research is focused on a history of biometric registration in South Africa, and he has recently published in *History Workshop* and the *Journal of Southern African Studies* on this subject.

Cheryl L. Brown, an Associate Professor of Political Science, teaches Internet Law and Policy, Cyberspace and Politics, Digital Forensics and Policy, and Politics of

China at the University of North Carolina at Charlotte in the USA. She received a National Science Foundation Award to study the formation of networks in cyberspace in the age of electronic government. Cheryl has conducted extensive research on information and communication technology in the Asia Pacific and published an article on smart card technology for e-government.

Andrew Clement is a Professor in the Faculty of Information Studies at the University of Toronto, Canada where he has coordinated the Information Policy Research Programme since 1995. He is a co-founder of the Identity Privacy and Security Initiative. His recent research has focused on public information policy, Internet use in everyday life, digital identity, information rights, public participation in information/communication infrastructure development and community networking. Clement is the principal investigator of the Digital Identities Construction project, as well as the Office of the Privacy Commissioner funded CAN-ID – Visions for Canada's Identity Policy, research project.

Simon Davies is Founder and Director of the watchdog group Privacy International and is also a Visiting Fellow in the Department of Information Systems of the London School of Economics and Political Science, UK. He works on privacy, data protection, consumer rights, policy analysis and technology assessment, and his expertise is in identity and identity systems. His publications include *Privacy and Human Rights 1998: An International Survey of Privacy Laws and Developments* (with David Banisar, 1998) and *Big Brother: Britain's Web of Surveillance and the New Technological Order* (Pan Books, 1997).

Kelly Gates is an Assistant Professor of Media Studies at Queens College, City University of New York in the USA. She teaches courses on media law and policy, the history of media technologies, and theories of the information society. She has published several articles on biometrics, and is currently writing a book on the politics of facial recognition technology.

Graham Greenleaf is a Professor of Law at the University of New South Wales, and formerly Distinguished Visiting Professor (2001–2002) at the University of Hong Kong. His research interests include privacy law and policy, commons in intellectual property, and free access to law. He is Asia-Pacific Editor of the bimonthly *Privacy Laws & Business International*.

Gus Hosein is a Visiting Senior Fellow at the London School of Economics and Political Science. At the LSE, he co-mentored its research into the UK Identity Card Bill. Subsequently, he co-founded the Policy Engagement Network that continues to bring academic research to policy fora. He is a Senior Fellow at Privacy International and Visiting Scholar at the American Civil Liberties Union. For more information, see http://personal.lse.ac.uk/hosein.

Zeinab Karake-Shalhoub is the 'Director of Research' at the Dubai International Financial Center (DIFC), PO Box 74777, the United Arab Emirates. Before that

Zeinab was a Professor of Business in the School of Business and Management (SBM) at the American University in Sharjah, UAE; she also served as the Associate Dean of SBM for five years. She is the author of five books: *Technology and Developing Economies* (Praeger Publishers, New York, 1990), *Information Technology and Managerial Control* (Praeger Publishers, New York, 1992), *Organizational Downsizing, Discrimination, and Corporate Social Responsibility* (Quorum Publishers, New York, 1999), *Trust and Loyalty in Electronic Commerce: An Agency Theory Perspective* (Quorum, New York, 2002), and *The Diffusion of Electronic Commerce in Developing Economies*, coauthored with Sheikha Lubna Al Qasimi, UAE Minister of Economy (Edward Elgar, November 2006).

Laurent Laniel is a sociologist of international relations and a Research Fellow at the Institut National des Hautes Etudes de Sécurité (INHES) near Paris, France. His research interests are international trade of illicit drugs, policing, and identification. He was a member of UNESCO's MOST-drugs network between 1997 and 2002 and co-author of the MOST-Drugs final report, *Drugs, Globalization and Criminalization*. He is the author of many papers and translations on the international drug problem and law enforcement. Most of his writings and photographs are available at http://laniel.free.fr.

David Lyon is the Director of the Surveillance Project and Research Chair in Sociology at Queen's University, Canada. Professor Lyon has been working on surveillance issues since the 1980s, and has particular research interests in national ID cards, aviation security and surveillance and in promoting the cross-disciplinary and international study of surveillance. His most recent books are the edited collection *Theorizing Surveillance: The Panopticon and Beyond* (Willan, 2006) and *Surveillance Studies: An Overview* (Polity, 2007). He is currently preparing *Identifying Citizens: Software, Social Sorting and the State* for Polity Press (2008).

Willem Maas (PhD, Yale) is Assistant Professor of Political Science at Glendon College, York University and previously spent three years at New York University, where he was Assistant Professor of Politics and European Studies. He has been a Parliamentary Intern and also worked at the Privy Council Office in Ottawa and the European Commission in Brussels. Professor Maas' teaching and research focus on comparative politics, European integration, citizenship and migration, sovereignty, nationalism, democratic theory and federalism. He is the author of *Creating European Citizens* (Rowman & Littlefield, 2007).

Taha Mehmood is trained as a media practitioner. His areas of interest include the history of surveillance, work practices of new economy labour, urban studies and film. His chapter stems out of his research with the Information Society Project at SARAI CSDS, Delhi, India. He is currently pursuing his Masters in City Design at London School of Economics.

Midori Ogasawara worked for Japan's national newspaper, *Asahi Shimbun*, from 1994–2004. As a reporter, she covered surveillance issues including national

identification card systems, CCTV in public spaces, war compensation between Japan and Asian countries, especially sex slavery on behalf of the Japanese army, and other human rights issues. She is also the author of four books including a children's picture storybook, *Princess Sunflower*, which is based on the Convention on the Elimination of All Forms of Discrimination against Women. She has been a MA student in Sociology at Queen's University in Canada since 2005.

Pierre Piazza is a lecturer in political science at Cergy-Pontoise University near Paris, France. He is a specialist of the social history of state identification systems and techniques and has published several papers on the Bertillon system (anthropometry), finger printing (dactyloscopy), identity cards and biometrics. Piazza is author or editor of *Histoire de la carte nationale d'identité* (*A History of the French National ID Card*), (Paris, Odile Jacob, March 2004), 'Police et identification. Enjeux, pratiques, techniques' ('Policing and Identification: Issues, Practices and Techniques'), and *Du papier à la biométrie. Identifier les individus* (*From Paper to Biometrics: Identifying Individuals*), (Paris, Presses de science, June 2006).

Jeffrey M. Stanton (PhD, University of Connecticut, 1997) is Associate Dean for Research and Doctoral Programs in the School of Information Studies at Syracuse University. Dr Stanton's research focuses on organizational behaviour and technology, with his most recent projects examining how behavior affects information security and privacy in organizations. He is the author with Dr Kathryn Stam of the book, *The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets – Without Compromising Employee Privacy or Trust* (*Information Today,* 2006).

Scott Thompson is a PhD candidate in sociology at the University of Victoria and is currently engaged in research concerning surveillance, classification and its consequences during the pre-electronic period. He has published several papers on surveillance and liquor control in Ontario, Canada and is currently writing a book with Dr Gary Genosko tentatively entitled *Punched Drunk: Alcohol, Identity and Surveillance in Ontario 1927–1975* (Forthcoming).

David Wills is a final year doctoral student at the University of Nottingham, and will be taking up a Research Fellowship at POLSIS, University of Birmingham, UK. His research interests include political theory, social movements, and the politics of information technology. He has taught political theory at Nottingham and wrote the POSTnote on Computer Crime for the Parliamentary Office of Science and Technology in 2006.

Dean Wilson is a Senior Lecturer in Criminology in the School of Political and Social Inquiry, Monash University, Melbourne, Australia. His research interests include the impact of biometrics on border control, police interactions with victims of crime, and the role of surveillance in the structuring of security. He has published widely on policing, CCTV in Australian public spaces and biometrics. He is the Oceania editor for the online journal *Surveillance & Society* and the editor (with Clive Norris) of *Surveillance, Crime and Social Control* (2006).

3 The elusive panopticon

The HANIS project and the politics of standards in South Africa

Keith Breckenridge

> Imagine it.
>
> A secure, single means of identification for 43 million citizens.
>
> Done.
>
> South Africa's Department of Home Affairs partnered with several contractors, including Unisys, to develop the Home Affairs National Identification System (HANIS) one of the world's largest civilian fingerprint databases.
>
> (Online. Available: http://www.unisys.com)

More than a decade ago the South African Department of Home Affairs issued a tender for the building of an Automated Fingerprint Identification System (AFIS), a database system for the biometric data that would integrate with the existing Population Register, and the issuing of identity cards to the entire population. Some of the elements of the Home Affairs National Identification System (HANIS) have been implemented, but South Africans are still waiting for their new identity cards. In the meantime, the Home Affairs Department – the division of the state that provides citizens and foreigners in South Africa with all of the essential documents of identification – has spun slowly into administrative collapse. This chapter is an attempt to explore the reasons for the HANIS debacle; I also want to consider another question, which may be of interest to those who live far from South Africa: Can a centralized and interoperable system of biometric identification actually be implemented? Or, to use the words of our contemporary theory, is the biometric panopticon possible?

The significance of HANIS

The South African biometric project is often used as a precedent for the biometric identification systems that are now currently underway in many liberal and social democracies. When the CIA's John Woodward, the leading policy advocate of administrative biometrics, began to map out their possible uses in government in 1997, he used South Africa and the Philippines as examples of societies that had resolved to introduce a biometric national identification card. Similarly, when the

(Conservative) British government began to re-consider the introduction of a national identity card in 1996, journalists pointed to the South African grants system as the single case that combined both the new smart card applications and identification technologies. The stories in the British financial press, which described the extension of the cutting-edge of banking technology to some of the most underdeveloped regions of Africa, gave the South African story particular power. Here was an excellent example of the use of biometrics for purely civilian and humanitarian ends. After 9/11, as the western democracies scrambled for a bureaucratic remedy to the danger within, the South African HANIS project was widely cited as an example of nationwide civilian biometric smart card identification. Recently, the global IT conglomerate, NEC, has used its involvement in the South African project as evidence of its suitability for selection as the provider of biometric border control systems in Britain (NEC Corporation 2006). In the effort to build support for a biometric smart card to control access to government health and welfare benefits, the Australian government used the example of smart card usage in Finland, France, Germany, Italy, Taiwan and South Africa. As *Electronic Frontiers Australia* has noted, of the countries cited as precedents, only the South African HANIS project includes the three elements of photographic identification, biometric registration and smart card applications (*Electronic Frontiers Australia* 2006). As the United States' Department of Homeland Security has become preoccupied with building an integrated global biometric surveillance system, the complexity of the HANIS experiment needs, I think, to be more widely understood than is currently the case (Chertoff 2007).

South Africa is, of course, a special society. For decades, scholars have studied it as the capstone of the system of racial capitalism that developed in the Atlantic world after slavery. In the years since the democracy began in 1995, and following the demise of formal segregation in the Americas, some of this significance has dissipated. As I have suggested elsewhere, in an era of increasingly centralized and coercive surveillance, the South African state is important because it is the first example of a truly biometric order (Breckenridge 2005a). Much of what the advocates of biometric registration systems around the world have been calling for since the start of the War on Terror has already been implemented in South Africa.

Some features of this society deserve special mention. The bureaucracy in South Africa is very radically centralized, especially in relation to the processes of vital registration. All births, marriages and deaths are recorded by the Department of Home Affairs in Pretoria: the state delegates no registration functions to local or provincial government. The same pattern is true of drivers' licences, passports and the primary tool of identification, the ID book, which are also issued and registered centrally. (There is also only one centrally controlled police force.) Interlaced with this intensely centralized bureaucracy, is a pervasive reliance on fingerprints for official identification. For much of the twentieth century, the South African state sought to use large scale fingerprint registers to control the movements and identity of African, Indian and Chinese people. This enthusiasm for administrative biometrics reached its apogee in the 1950s when Hendrik Verwoerd built a single,

centralized fingerprint repository called the Bewysburo – or the Bureau of Proof – into the foundations of the Apartheid state (Breckenridge 2005b). In the decades that followed, some of the key functions of the central government were dismantled under the policy of Bantustan self-government, but since the early 1990s, the energy of centralization has been revitalized. Today all South Africans have a biometrically authenticated official record of identity, and millions of people make daily use of their fingerprints in their dealings with the government. This means that the South African biometric identification project, quite unlike the cards currently being considered in other countries, had a multifunctional character from the outset: the designers of the HANIS system intended it to function as a biometric panopticon.

On the face of it, then, the history of biometrics in South Africa is a special instance of Foucault's now very widely used theory of biopolitical government (Burchell et al. 1991). In fact, I think, the theoretical importance of HANIS may lie elsewhere. In the first instance, I would like to reaffirm the scholarly significance of specific regional and temporal details in the face of what is very often a circular and derivative interest in the power of Foucault's analysis of the discourse of the subject. In asserting the significance of this South African history, I want to resist the tendency to relate it to a handful of metropolitan theorists and scholars, a very common analytical move which tends to ignore the specific, and difficult, histories and historiographies of this region, and many others. Similarly, I want to show that the fractures and contradictions that obstruct the development of biometric surveillance are at least as important, politically, as the imperatives of convergence.

The origins of the HANIS system lie over a century ago when the founding figure of administrative fingerprinting, Sir Edward Henry, spent six short months on the Witwatersrand between his appointments as Inspector-General of the Bengal Police and Deputy-Commissioner at Scotland Yard (Sengoopta 2003). Following the suggestion that Francis Galton had made in his book *Fingerprints* in 1891, Henry's repositories were very rapidly put to use as tools of labour recruitment and control. This dependence on coercive systems of labour mobilization culminated in Verwoerd's grand project for a centralized biometric identification register, and the infamous Dompas pass system. In the decades that followed this system of control was applied to all South Africans.

The immediate causes of the HANIS system lie in the national security concerns of the South African state in the early 1980s, in particular the decision by PW Botha's government in, January 1981, to issue a single, fingerprint authenticated, identity document to all South Africans, white as well as black. In the preceding year the African National Congress's special operations unit, under the command of the white communist, Joe Slovo, had staged flamboyant attacks on the fuel refineries in Secunda and Durban. These attacks coincided with Botha's energetic militarization of the South African state (Cock and Nathan 1989). Key members of the government, like Chris Heunis, the new minister of the Department of the Interior, had begun to set in place a constitutional order called the National Security Management System that re-drew the lines of political authority around a set of

regional committees dominated by the South African military (O'Meara 1996: 255–269). The military and its Cabinet supporters argued that South Africa faced a Soviet-sponsored 'Total Onslaught'. Establishing a national fingerprint register of all white, Indian and coloured South Africans was one of the key elements of the 'Total Strategy' they had designed to preserve white power. On the day of the Minister's announcement, a spokesman for the South African Defence Force explained that the military believed that it was necessary to 'upgrade the sophistication of identity documents'. In 1981, as the *New York Times* observed at the time, the fledgling biometric access control technology was 'a solution to a problem that no one's aware of yet'. With the decision to set up universal fingerprint identification as an anti-terrorist strategy the South African government was creating the *raison d'etre* of the newly christened biometric access control industry.

Many white people, especially those who had the original *Book of Life* issued in the 1970s, did not apply for the new, fingerprinted, identity document until the deadline approached in 1990, the same year that the African National Congress was unbanned. There is some irony in the fact that thousands of white South Africans queued to be fingerprinted for ID books designed as an anti-terrorist measure, and instrument of white racial supremacy, in the year after Nelson Mandela was released from prison. By this time, officials had begun to stress different reasons for holding the books, like the usefulness of fingerprints for 'orderly public administration', for business or for identifying dead bodies, but the desire for closure, for completing the national register, had now become both the end and the means of the state's policy (Brits 1990; Stirling 1988).

The HANIS project also has roots in the intensely-contested debate about the character of the post-Apartheid welfare system. The first meaningful discussions for a biometric identity card took place in 1994 during the inter-departmental planning for the implementation of the ANC's first economic and social policy, the 'Reconstruction and Development Program' (RDP). The RDP expressed the economic policy goals of academics and activists associated with the internal political organizations, unions and civics, and at its core it was an argument about the provision of basic services and welfare benefits to millions of very poor South Africans (Marais 2001: 122–159; The Reconstruction and Development Programme 1994; Bond 1996). The Home Affairs representatives on this committee, Piet Fourie and Peter Payne-Findlay, were saddled with the responsibility of ensuring that the benefits were fairly distributed amongst the potential beneficiaries, and that only South Africans would qualify. The grants, land, housing and basic service reforms envisioned for the RDP would involve a much larger group of recipients than the 20 million people then being recorded in the Population Register (although they probably did not have in mind a doubling of the size of the database). With the huge amount of work involved in the processing of fingerprints in mind, they proposed that Home Affairs should implement an Automated Fingerprint Identification System and an identity card. Payne-Findlay persuaded the Director-General to support this idea and he was given the task of drafting the proposals for the AFIS. Over time, this task expanded into requests for proposals from the largest international computer companies for the three different parts of the HANIS system: the AFIS, the cards

and the building of the Home Affairs computer systems. Payne-Findlay drafted the R800 million tender that was announced by the Minister in December 1996 (Informant 8 2007).

The announcement of the HANIS project catapulted Home Affairs back into the limelight of the international government computing industry. After decades of being international pariahs, the Home Affairs officials and their new ANC political leaders, were being feted by the largest multinationals. The list of IT companies tendering on the South African project was a Who's Who of international government computer contractors: TRW, Sagem Morpho, Unisys, ICL, Olivetti, Printrak, Labat-Anderson, Lockheed-Martin, Marubeni. Each of these firms set up complex joint ventures that brought in local companies closely associated with the old state – Denel, Plessey, Persetel-Qdata and a string of Empowerment partners, the South African term for companies controlled by black shareholders – Don Ncube's Real Africa Holdings, Bhekisizwe Computer Systems, Robert Gumede's Gijima Holdings. Here was a potent political cocktail indeed (Lunsche 1997, 1998; Stones 1997; Delaney 1998a,b).

Each of the companies bidding for the HANIS contract approached the task of convincing the tender board in a different way, but the overall effect was to suggest that in adopting biometric identification, South Africa was joining the cutting edge of international bureaucratic practice; the tender process nicely demonstrates the ways in which states and private contractors work in an intrinsically international field of practice. A special representative from the British Home Office where, in Buthelezi's words, 'much progress with the implementation of an automated fingerprint system has been made', assisted in the evaluation of the proposals (Buthelezi 1997). Lockheed-Martin traded heavily on its experience as the AFIS contractor for the FBI's similarly sized repository of 40 million fingerprints. Sagem Morpho, the massive French defence corporation that dominates the global market in digital fingerprint readers, emphasized its role in the large scale biometric ID projects then under development in Honduras, Philippines and, most importantly, Malaysia. When Unisys wanted to demonstrate the usefulness of their systems they had a clear advantage in that they could present systems actually in place in South Africa. The evaluation committee was invited to tour the California prisons system to view the Unisys tools at work and, drawing on the longer history of Datakor, its sanctions-era subsidiary inside the country, they visited the Lindela Repatriation Centre and another local juvenile detention facility to observe biometric identification at first hand.

The first real shock came a year later with the elimination of the major international biometrics companies in the second round of the evaluation process. The two consortiums left in the race were both dominated by older South African firms: QData/Persetel were opposed by the Marpless Consortium (consisting of Unisys, Plessey, Marubeni and Gijima). The consortiums dominated by Lockheed-Martin and Sagem complained vociferously to the press, the State Tender Board, the Auditor-General and the Parliamentary Portfolio Committee that their exclusion imperiled the entire project. ICL's local representative hinted at underhand dealings when he protested that Sagem's AFIS had never 'been disqualified prior to

benchmarking in the context of international open tenders'. Even the French Ambassador lobbied the Minister to review his decision not to grant the tender to Sagem (Delaney 1998a; Buthelezi 1998).

Under this pressure, the Parliamentary Portfolio Committee duly subjected Payne-Findlay to a grilling. He was publicly accused of tampering with the HANIS tender, and stripped of any decision-making authority over the project. Sagem commended the Parliamentary Committee, thanking them for 'doing a good job in investigating our complaints'. These complaints precipitated the first significant delay in the evolution of the HANIS project. At the Committee's suggestion, both the Auditor-General and the Public-Protector initiated investigations into the tendering process. Six months later, in December 1998, the Protector's report found no significant problems. A contract was signed with the Marpless Consortium in February 1999 (Delaney 1998; Buthelezi 2002).

Behind the scenes the actual content of the contract began to change almost immediately; most importantly the physical and technological features of the card were dramatically altered. One key change was the decision to use NEC fingerprint verification equipment in the final version of the Marpless proposal. Another was the later decision, subsequent to the awarding of the tender but before a contract was signed, to abandon the bar-code equipped cards provided by Polaroid. This decision to move to smart cards was critical, for it opened up a wide field of theoretical possibilities for HANIS, turning it from a dual-purpose identification and electronic purse project into a multi-purpose vehicle for the state's many information processing requirements. In practice it also meant that the HANIS project was awarded without a card issuing contract.

The decision to abandon the bar-coded cards came before the granting of the tender in March 1999. It was later justified in the computer press as an obvious choice of new technologies over old, but the reasons for the shift to the smart card were more convoluted. Security is the most common reason for adopting smart cards in identification systems. It is the security of cards equipped with integrated circuits (because they can store and process the very large numbers necessary for public key encryption) that is conventionally offered as the explanation for the claim that biometric smart cards mark a qualitative change in the history of state identification systems. But in the late 1990s smart cards, because of their very limited memory and processing power, were not dramatically more secure than magnetic stripe cards.

The move to a smart card based identity card followed intense lobbying at the highest level of the state, leading to a meeting of the Directors-General to discuss the issue in April 1998. At this meeting, Andile Ngcaba, the Director-General of the Department of Communications and the ANC's key IT expert in the first decade of their rule, seems to have played the key role (Van den Heever 2001). The example of two contemporary Asian biometric identification schemes loomed large. 'South Africa has looked overseas for implementation models', *SA Computer Magazine* reported, 'to countries such as Malaysia, which recently rolled out one million smart cards to its population, and to Hong Kong, which announced its interest in swapping the two-dimensional bar code for the smart card' (Wright 2002).

A single view of the customer

Very soon after the decision to adopt the smart card, the Department of Home Affairs began to chart out the possibility of using the identity cards to host all of the key functions of government information processing. No longer a single-purpose tool of identification, the card had now become the lynch-pin of a host of bureaucratic and commercial functions. 'The smart card that we are introducing is not confined to the limited identification/verification realms of the Home Affairs strategic engagement only', Minister Buthelezi announced to the media in February 2000. 'Rather, it is a magnanimous, multi-applications, government smart identity card with extensive capabilities contained in a chip that boasts enough intelligence to allow other departments and perhaps even other forms of industry permissions to utilize the card technology' (Buthelezi 2000). With a prospective budget for the smart cards now being proposed at the nice round number of R1 billion – some 25% more than the entire project was originally estimated to cost – the Department began to gather the different commercial and bureaucratic interests that might want to use them. An inter-departmental committee, involving over a dozen different departments and staffed by the most powerful officials in the national bureaucracy, began to consider the possibilities for the new smart card. In the early stages of the process there was widespread enthusiasm from these different departments for the HANIS smart card. Gareth Warner, who had taken over from Payne-Findlay as the outside consultant of the HANIS project, remembered that, at this time, 'everyone had the same issues' (Warner 2007a).

With encouragement from an enthusiastic and very powerful inter-departmental committee, Home Affairs began to look around at the most common transactions in the other departments; very early on it became clear that the success of the card would lie in two areas: banking and welfare. Early in 2000 three separate teams were appointed: the first looked at existing smart card systems inside the country like the millions of GSM cards in the exploding cellular phone market and the proprietary system used by Aplitec to deliver pensions and other grants; the second was charged with the investigation of a set of technical specifications for the cards; and the third considered the possibilities and mechanisms for making the cards interact with the existing card infrastructure (Whitby 2000). Right at the outset the success of the cards was tied to tight integration with the requirements of the social grant system and the emerging Europay–Mastercard–Visa standard that promised access to the robust and extensive banking network. Buthelezi stressed both goals in his parliamentary briefing, just weeks after the Marpless contract was signed, when he explained that the interdepartmental committee had 'decided to honour our senior citizens with the privilege of being the first beneficiaries of this world class project', which would give them the 'ability to draw, should they elect to do so, their grants from bank ATMs using their smart cards' (Buthelezi 2000a).

By the middle of 2000, under the general influence of the fast waning dotcom frenzy and the particular encouragement of Andile Ngcaba, the smart card had grown into an instrument of digital social transformation. During the month of August, Home Affairs called for proposals from businesses for applications on the smart card. The response, in the Minister's words, 'was overwhelming with more

than 50 companies and interested parties submitting responses'. In the wake of these proposals the department began to argue that 'e-governance and e-commerce will be closely coupled to the envisaged identity card'. In these months, the role envisaged for the cards expanded from 'key enabler' to a dozen government departments into a general purpose instrument of electronic commerce. Adopting and extending the role of the current population register, which is accessed by the banks and insurance companies for official confirmation of death, the biometric HANIS cards would provide businesses with a foolproof mechanism of identity. 'The card', Buthelezi promised, 'will eventually be used by a number of private organisations such as banks, insurance companies, medical aid schemes and many more, to combat fraud' (Buthelezi 2000c). Some 18 months later, at the commissioning of the Marpless system, the Minister's sense of the pool of commercial users had expanded to include 'any branch of government and any private entity which adopts the system required to read it electronically'. The biometric smart cards, in this scheme, would deliver automated access control across the borders of the country and 'building access control or by vending machines which intend to restrict their products, such as cigarettes, to adults only' (Buthelezi 2002).

As the range of possible users for the smart card expanded so did the Department's sense of the cards' function as the lynch-pin of all state activities. Holding out the triple promise of automated record keeping, public key encryption and biometric authentication, the smart cards seemed to realize the project of the original Book of Life, providing a secure, single record of the citizen's entire engagement with the bureaucracy. With proposals from over a dozen departments, the Interdepartmental Technical Committee began to plan for the smart card itself to coordinate and record the dozens of different transactions between the departments and citizens (and non-citizens). After more than a year of discussions about the possible uses of the card the Committee sent the first of many proposals to the Cabinet. 'The vision', Patrick Monyeki explained, 'is that the smart card should provide the single interface between citizen and government'. Indulging the fantasies of corporate customer relations systems developers for a single summary record of the huge pool of electronic transactions swamping businesses, he implied that the cards would provide the state with a focused lens into the life of any individual. 'Envious corporates will note that this will, in theory at least', *Computer Week* told its readers, 'give government the elusive "single view of the customer"' (Van den Heever 2001).

The elusive panopticon

Monyeki's claim that the proposal for the card tender had been sent to Cabinet was the first of half-a-dozen similar claims that would be made over the next five years. In fact there was no technical mechanism to actually implement the grand project that the Interdepartmental Committee then had in mind. In November 2001, six months later, Home Affairs gathered together the most important actors in the emerging field of biometric smart card authentication to consider the difficult problem of the competing and incompatible technical standards offered by the different

biometrics companies. The problem was the same one that has bedevilled fingerprint classification and storage in general, and the construction of centralised registries in particular, since the turn of the twentieth century: no uncontested standard existed for smart card fingerprint identification, either in South Africa or internationally. 'Each respective manufacturer is offering his own preferred system as the ultimate solution', Gareth Warner warned, 'while the respective international committees push forward on the development of biometric standards which are still a long way off in terms of the development of comprehensive specifications' (Peachey-Warner 2003).

The situation presented a special problem in South Africa precisely because fingerprinting was so common. Drawing on the half-century of fingerprinting in the Central Reference Bureau, many other Departments had adopted fingerprinting as their preferred means of identification, and they had begun to purchase electronic solutions to automate the work of authentication and storage. At least five separate nationwide systems had been adopted by different government Departments in 2000: police, social welfare, drivers' licensing, and the courts and prisons had all already purchased massive biometric systems, each with millions of records, independently of Home Affairs. Some departments, like Social Welfare, had contracted different companies to undertake the work in each province. 'Currently five provinces use smart card technology coupled with fingerprint biometric technology to pay out state grants', Warner wrote at the time 'and there is no development of common standards across these provinces both in terms of smart cards and fingerprint biometrics' (Warner 2001: 13).

In some cases, this absence of standards created exactly the same problem as the early 20th century conflicts over modifications of the Henry system, but the new format also created new, even more intractable, difficulties. In the large scale AFIS systems, designers would create subsets of records that were obviously similar in order to avoid the necessity of undertaking matches across millions of records, using the arches, loops and whorls of Francis Galton's original classification (Warner 2001). Differences over the rules for the implementation of these clusters of records could build exactly the same classification incompatibilities into electronic systems as existed in locally customized manual registries.

A more serious problem has its roots in the huge difference between the electronic storage required to retain the original fingerprint and its mathematical template. The advocates of smart cards often play up their computational powers in deeply exaggerated terms; in fact the cards have very limited capacity. These physical limits on the storage available on the cards are aggravated by the budget constraints of large scale identification projects: the cards used in national identity cards tend to be the cheapest and smallest. When the HANIS project adopted the smart card format they were planning on 8 kilobytes (Kb), or at the most 16 Kb of memory. The significance of these physical memory limits becomes obvious in the context of the storage requirements of a normal fingerprint image. The compressed image of an individual fingerprint requires some 20 Kb of electronic memory, which means that even the largest and most expensive smart cards can accommodate only one or two complete fingerprint images. Even the oldest cards have

enough space to store copies of the mathematical representation of a fingerprint, called a minutiae template like Galton's original fingerprint classifications, these templates express the geometrical relationships between a limited number of details (or minutiae) from the dense patterns of individual fingerprint lines – the location and the direction of ridge endings, splits, loops (Information Technology Laboratory, NIST 2000). These are recorded numerically and combined in a carefully ordered sequence in to a single large number, which despite its complexity, takes up less than 250 bytes of memory – the mathematical template uses just 1 per cent of the memory used to store the image.

The immediate result is that all of the dominant manufacturers of biometric identification systems store only the templates on their cards. Each of these companies uses its own proprietary system of minutiae for encoding and interpreting the template on the card (Peachey-Warner 2003). This is potentially very problematic because, until recently, the different commercial systems could not interpret each other's templates, nor can the original print be reconstructed from the mathematical template. But it is catastrophic where, as is definitely the case with some of the social welfare grants systems developed by Aplitec, the original image is not retained at the database end. These problems of classification are not specific to South Africa; the same problems have also affected the US military in Iraq, another site of ubiquitous fingerprint registration (Gerth 2004).

Digital technology also introduces another problem that had not much troubled manual fingerprinting. 'Manufacturers of fingerprint scanners currently cannot deliver convincing evidence that they can make a distinction between a real, living finger and a dummy constructed of silicone rubber or any other material', Warner reported. For those companies planning to use and sell unattended biometric readers, a reliable mechanism to test for what he called 'liveness', was evidently a matter of some urgency.

The Biometric Standards workshop that Billy Masetlha hosted in November 2001 was called to address this 'grave challenge to government'. Home Affairs brought the main state contractors in South Africa – NEC, Sagem, Siemens and Oberthur card systems – together to plan the development of a local standard for the exchange of fingerprint templates between smart cards. Aside from the now glaring problems of incompatible proprietary systems, the Department returned to the idea that a properly designed smart card system could revolutionize both state and commercial transactions. The development of the local standard would make possible 'electronic interchange of biometric identifiers between government jurisdictions and commercial service providers requiring positive and secure methods of person identification of individuals'. The workshop came to rapid agreement on the specification of the image size and quality, but then quickly became mired in the conflicting systems of minutiae that each company used to generate the key produced from that image. The last resolution of the workshop set up a special committee under the control of the South African Bureau of Standards and the Council for Scientific and Industrial Research to work on a 'national biometric standard' compatible with the emerging international standard. 'Gone are the days when you can run to a province and sell each one a different product that does not

conform to a national standard', Patrick Monyeki warned the contractors (Dudley and Otter 2001).

Over the course of the next 18 months, two major agreements seemed to put in place the standards that were required to make HANIS work as the lynch-pin of a revolutionized networked society. Under Warner's influence, the different manufacturers, and their government clients, agreed to a standard fingerprint image format and they drafted a local standard for the sequencing of biometric data on the cards, called ARP 054, closely modeled on the standard then being developed in the USA by the National Institute of Standards and Technology. Home Affairs announced that this new local standard would be 'modified in the near future' to 'include an ameliorated definition of minutiae points and location' (South African Department of Home Affairs 2003).

Five years later a practical standard for biometric devices was still not available. Each of the major companies involved in the field of fingerprinting in South Africa retained its own system of minutiae for producing the numerical template. 'We could never come down to a biometric standard', Gareth Warner noted in 2007, 'each of the companies still uses a proprietary system' (Warner 2007b). Under pressure from the new US Homeland Security laws, international standards making bodies worked energetically in the years after 2003 to create templates that would allow the different commercial systems to exchange information reliably, but these new methods are still not 'defined well enough to allow for practical interoperability' (Warner 2007b). The HANIS project's dilemma derived from the fact that it could not, given the pervasiveness of biometrics in South Africa, adopt a single-supplier, fully proprietary system, like those being developed by Sagem around the world, and it preceded, probably by decades, the emergence of a practical interoperable standard for biometric devices.

The companies involved in the provision of biometric identity cards, particularly Sagem Morpho who claims to have captured '1.5 billion fingerprints worldwide', have very good reasons to resist the development of an effective open standard (Hi-Tech Security Solutions 2004). The most obvious of these is that they earn a licence fee for the proprietary template for every card issued over the lifetime of the identification system; revenue that will very likely last for a generation. In addition to those fees, the nationwide adoption of a single, proprietary minutiae template would mean, as Monyeki and Warner warned in 2001, that the state is forced to pay for hardware from the supplier who owns the license for the lifetime of the cards. In South Africa, and internationally, Sagem occupies a formidable position in the economy of identification, and it is vigorously supported by the diplomatic resources of the French government. The company's contract for the AFIS system used by Interpol gave them an inside track on the tender for the South African Police Services Criminal Records Centre. Sagem also sell the mobile Morphotouch machines that are widely used by the police and the private social welfare grant delivery companies to search for fingerprint matches. When the HANIS contractors built a smart card production facility, they duly chose Sagem equipment and templates. But this system was never used to produce cards, because of Home Affairs' desire to coordinate the HANIS system with the other existing biometric systems using an open standard.

Under pressure from the US government, the most powerful international standards-making bodies worked busily after 2001 to compose an interoperable standard, but the results of these efforts were complex, and they came, in any case, much too late for HANIS (International Committee for Information Technology Standards 2003). The political and financial energy behind this movement towards an open standard for fingerprint minutiae was unmistakable: all of the documents cite US Department of Defense, Patriot Act or Presidential Homeland Security directives citing the same concerns for interoperability that had troubled the South Africans in 2001. Two issues loomed large in these workshops: the first was avoiding vendor lock-in, or technological dependence on a proprietary standard, and the second was the digital panopticon or interoperability, the goal to make all biometric devices interact with each other. Under this pressure the major biometrics contractors had agreed by March 2004 on a basic open standard for biometric minutiae, INCITS 378.

The tests that the US government commissioned of the open standard in 2005 have some startling implications for the project of an interoperable biometric identification system (National Institute of Standards and Technology 2006). These investigations were undertaken on millions of fingerprints taken from the largest digitized collections in the USA, which means that they do not address the first difficulty of fingerprints that resist templating altogether. The massive tests showed that the use of the INCITS standard in place of the three most accurate, proprietary systems (produced by the dominant companies NEC, Cogent and Sagem) doubled the rate of incorrect rejection (False Non-Matching), and produced a ten-fold increase in the much less likely errors of mistaken identification (False Matching). If, in other words, the open standard was used on the most accurate matching systems to test the identity of 1,000 people it would falsely reject twice as many people as the proprietary system (20 instead of 10). It would, also, incorrectly identify one or two people out of every 1,000 where the proprietary systems would be unlikely to do that in a population of 10,000.

The obvious remedy for the increased rate of error produced by the open standard was to move away from a single biometric measurement to multiple indicators. This, in turn, raises a host of new incompatibilities for already existing biometric systems. Some of these have only recorded a single biometric, while others, like the Aplitec biometric smart cards, have selected the best fingerprint impressions on a case by case basis. The use of an open template on multiple fingerprints would first require agreement on the fingers being captured, with very onerous administrative implications for the already existing systems that do not meet this requirement.

The obvious question is this: did the HANIS project fail solely because it preceded the development of a viable system of biometric surveillance? Will subsequent schemes work more effectively? Certainly, the current drive to biometric convergence is intensive, with the political and economic pressure of powerful divisions of the US government leading the most important technology corporations towards an open standard, and it is extensive, with institutions in Europe and the USA working in an independent but coordinated project. But the movement to an interoperable standard, and with it the project of the biometric panopticon, is

also strongly contradicted by the technological and administrative consequences of an open system. For the largest companies (especially Sagem Morpho) the goal of locking national identification systems into a proprietary system remains a very attractive and viable project. The most likely outcome, in the context of very vigorous lobbying, is that the proprietary systems will prosper, interacting with the open standard in a fashion that remains subject to significant rates of error.

Banking on standards

The difficulties that the HANIS developers faced in securing an interoperable standard for fingerprints were mirrored in another key aspect of the biometric panopticon: the development of a smart card standard for the banking system. From early in 2000, Home Affairs worked with representatives from the banking industry to map out the electronic payment systems that would be required for the HANIS smart card to meet the requirements of the Europay–Mastercard–Visa standard for the banking infrastructure. In June of that year, all of the major South African banks agreed to implement the EMV standard for payment systems, which was, at that stage, nearly a decade old. In these discussions the banks appeared to be working to a deadline of January 2005 for the introduction of a nationwide system of ATMs and point of sale machines capable of reading the smart cards (South African Department of Home Affairs 2003).

The commercial banks proved much slower than anyone had predicted in adopting the EMV smart card standard. By the middle of 2007, more than two years after the agreed deadline, most of the banks were still using the magnetic stripe technology, and they had scarcely begun the massively expensive project of replacing existing teller and point of sale machines. While the banks proposal, in 2003, for their own smart card based 'Account for Life' (Duminy 2003) seemed to run across the bows of the HANIS project, the real difficulty was that the functionality proposed for the HANIS card presumed a much higher degree of synchronization between the banks, and a much more urgent timetable, than was actually the case (Engelbrecht 2006). 'The banks were brought into the picture', one of the project manager's observed, 'but there was never a time that we actually reached a compromise as to what the card should actually contain' (Informant 8 2007).

Added to the difficulty of herding the banking cats was the even more sensitive problem of adopting fingerprinting in private banking. South African banks have been flirting with the use of fingerprint authentication for as long as the HANIS project has been under development (Engelbrecht 2006; *The Guardian* 1999; *Electronic Payments International* 1996). The same problems of proprietary technical standards threaten the banks but the real issue is that the banks are very nervous about public outrage over the adoption of fingerprint authentication. Without a statutory requirement that customers provide biometric authentication the banks were not likely to impose fingerprint checking on their customers, which meant that there was no immediate benefit for commercial fraud detection. By the beginning of 2007 the EMV standards-based electronic purse had been effectively abandoned as part of the HANIS project. When the Minister was asked if the Banks or the

Department had 'washed their hands of the smart card project', she pointedly responded that the 'Department had not' (Justice, Crime Prevention and Security (JCPS) Cluster briefing 2007).

Where the four major banks in South Africa have been very slow to adopt smart cards for individual financial transactions, the opposite has been true in the privatized field of social welfare payments. In these transactions, biometric authentication was ubiquitous as early as 1996, and by 2003 the field was dominated by a single company bearing its own patented smart card interchange standard and providing a massive network of point of sale devices across the continent. Aplitec, or Net1 UEPS to use its new Nasdaq trading name, is the brainchild of Serge Belamont, a Frenchman who developed the South African interbank ATM network in the late 1970s. His project is to build an anti-bank, a smart card-based financial system that makes almost no use of the existing banking network infrastructure, in order to deliver financial resources and products to the global poor. At the heart of this campaign, a deadly serious attempt to build a non-EMV financial empire, is the UEPS anti-standard for intercard data exchange. Aplitec shares this facility with no-one, not even their bureaucratic paymasters, as the cards themselves are the bearers of all the financial data required to track funds to individuals, merchants and the company (Net 1 UEPS Technologies, Inc 2006).

Since 1999, the company has grown spectacularly rapidly, attracting investments from the major banks and, more recently, a listing on the NASDAQ stock exchange. In the single year, 2004–2005, the stock price of Net1 rose 15-fold, reaching nearly US$1.5 billion (Sergeant 2005). In 2000, Belamont was asked about the threat to his business from the HANIS smart card. 'Government will separate the payment application from the ID card', he replied, 'and leave the payment card to the financial industry' (Lloyd 2000). He has proven surprisingly prescient. Aplitec has a history of sailing very close to the wind of government, but those who have been involved in the HANIS project see nothing underhand in the company's dominance. 'Welfare eventually gave up on us as they said we would never issue a card and that they had to pay out pensions', one of the manager's explained, 'how right they were' (Informant 8 2007). By 2007, Aplitec Net1 had some 4 million bearers of its biometrically authenticated smart cards for the delivery of welfare grants, and more than 4,000 point of sale machines capable of transacting only with those cards. The company has effectively constructed its own proprietary banking infrastructure and welfare payment system, fulfilling the two trophy projects of the HANIS smart card without any of its interoperability.

Conclusion

This study of the HANIS project suggests that a biometric panopticon that will allow states to monitor the movements and behavior of their citizens across the different fields of social life – migration, social welfare, banking, policing – is not currently possible. Indeed it suggests that biometric systems that are strictly targeted at a single set of transactions – healthcare or migration – are much more likely to work in the short term than the interoperable systems that national security policy

advocates have in mind (see Etzioni 2000: 103–37). It also seems likely that national identification systems that are wholly owned by one of the largest firms, like Sagem, Cogent or NEC, are likely to be much easier to implement and more efficient than an open system. Yet there are also unmistakable signs that the implications of this kind of monopoly for control of the means of identification are unacceptable to policy makers in all of the wealthiest states (see Torpey, the introduction to this volume).

It is also clear that the individual national debates about the costs and benefits of biometric identification cards form part of an integrated transnational field. On this political terrain, the most powerful actors are the multinational firms and multilateral standards making bodies. This South African example demonstrates the difficulties of an isolated national effort to shape this debate. The politics of biometrics is driven by arguments about globally acceptable practice and precedent. In this debate the move to a set of open standards is ongoing, but the global firms have lobbying, diplomatic and financial resources that are not available to the advocates of open systems. If, as seems possible, the OECD countries now withdraw from the project of introducing biometric identity cards, that will leave the global identification economy in the hands of its current incumbents, in particular Sagem Morpho.

This study of HANIS shows that the errors of classification that have plagued large scale fingerprinting systems since the end of the nineteenth century do not disappear in the digital world. The advocates of biometric technologies stress the efficiencies and high levels of accuracy of computerized systems. But it is important, especially in the context of large scale and interoperable systems, to emphasize that biometric systems are in fact prone to error. These errors may be failures to enroll, or they may be matching errors. The errors will certainly increase if multiple systems and larger populations are subjected to a single biometric test. What is critical is that the citizens affected by these errors must be provided with a means for challenging these mistakes without the indignity of losing well established rights of due process.

In the attempt to answer the question: Is a biometric panopticon possible? – I have been drawn to Bowker and Starr's characterization of the development of 'technical standards as a site of political decisions and struggle' (Bowker and Starr 1999: 49). In this conflict, the interests of modern capitalist firms and state bureaucracies pull in both directions, but so does history. Actually existing biometric systems have inherited the interests and associations of at least six politically very different axes in the twentieth century: imperial labour controls, prisons and policing, national security, social welfare, banking and computing. These systems are not naturally compatible, and in some respects they conflict directly. In the HANIS case the conflict between a tool designed for national security and the demands of the banking and social welfare systems have proven, to date, irreconcilable. It is these conflicts that have played themselves out in intractable difficulties over technical standards. Over time, the conflicts may diminish, producing the kinds of open standards that will allow for interoperable digital surveillance, but that day is still a long way off.

Bibliography

Bond, P. (1996) 'Neoliberalism comes to South Africa', *The Multinational Monitor*, May.

Bowker, G. and Starr, S. (1999) *Sorting Things Out: Classification and its consequences*, Cambridge: MIT Press.

Breckenridge, K. (2005a) 'The biometric state: the promise and peril of digital government in the New South Africa', *Journal of Southern African Studies* 31(2): 267–82.

Breckenridge, K. (2005b) 'Verwoerd's bureau of proof: total information in the making of apartheid', *History Workshop Journal* 59(1): 83.

Brits, E. (1990) 'Kwessie van ras en vingerafdrukke pla nog', *Die Burger* 15 June.

Burchell, G., Gordon, C. and Foucault, M. (1991) *The Foucault Effect: Studies in Governmentality*, Chicago: University of Chicago Press.

Buthelezi, M. (1997) *Min Buthelezi: Parliamentary Briefing – Sept '97*, 10 September. Online. Available: http://www.info.gov.za/speeches/1997/0916HOME97.htm (accessed 11 April 2007).

Buthelezi, M. (1998) *Budget Debate*, 14 May. Online. Available: http://www.info.gov.za/speeches/1998/98908_2459810879.htm (accessed 31 May 2007).

Buthelezi, M. (2000a) *Home Affairs National Identification System: Project Launch*, 31 January. Online. Available: http://www.info.gov.za/speeches/2000/000301503p1001.htm (accessed 31 May 2007).

Buthelezi, M. (2000b) *Parliamentary Media Briefing,* 10 February. Online. Available: http://www.info.gov.za/speeches/2000/0002111208p1001.htm (accessed 31 May 2007).

Buthelezi, M. (2000c) *Parliamentary Media Briefing,* 21 September. Online. Available: http://www.info.gov.za/speeches/2000/0009221010a1003.htm (accessed 31 May 2007).

Buthelezi, M. (2002) *HANIS Basic System Commissioning*, 18 February. Online. Available: http://www.info.gov.za/speeches/2002/0202191046a1001.htm (accessed 11 April 2007).

Chertoff, M. (2007) 'Remarks by Secretary Michael Chertoff to the Johns Hopkins University Paul H. Nitze School of Advanced International Studies', *Department of Homeland Security*, 3 May. Online. Available: http://www.dhs.gov/xnews/speeches/sp_1178288606838.shtm (accessed 8 May 2007).

Cock, J. and Nathan, L. (1989) *War and Society: The Militarisation of South Africa*, Cape Town: David Philip.

Delaney, Jeff (1998a) 'Failed HANIS bidders in the dark', *Computing SA*. Online. Available: www.computingsa.co.za (accessed 11 April 2007).

Delaney, Jeff (1998b) 'Hanis decision expected "shortly"'. Online. Available: http://www.ictworld.co.za/EditorialEdit.asp?Archive=1&EditorialID=2844 (accessed 21 April 2007).

Dudley, G. and Otter, A. (2001) 'Standards critical to State biometric projects, says', *ITWeb*, 21 November. Online. Available: http://www.itweb.co.za (accessed 11 April 2007).

Duminy, B. (2003). *Account for life – a feasibility assessment prepared for Finmark Trust,* May. Online. Available: http://www.finmarktrust.org.za/documents/2003/MAY/AFL_Report.pdf (accessed 11 April 2007).

Electronic Frontiers Australia (2006) *Australian Govt. Access Card – Comparison with Other Countries,* 26 May. Online. Available: http://www.efa.org.au/ Issues/Privacy/ac-intcomparison.html (accessed 24 April 2007).

Electronic Payments International (1996) *South Africa: Biometrics set to revolutionise banking*, 25 September.

Engelbrecht, L. (2006) 'Banking on biometrics', *ITWeb*, 17 November. Online. Available:

http://www.itweb.co.za/sections/quickprint/print.asp?StoryID=168621 (accessed 11 April 2007).

Etzioni, A. (2000) *The Limits of Privacy,* New York: Basic Books.

Gerth, J. (2004) 'Fingerprinting glitches are said to hurt antiterror effort', *New York Times*, 27 October.

The Guardian (1999) 'The eyes have it', 20 May.

Hi-Tech Security Solutions (2004) *Ideco Technologies – perfection in biometric technology,* October. Online. Available: http://securitysa.com/regular.aspx? pklRegularId=1860 (accessed 15 August 2007).

Informant 8 (2007) HANIS Project Employee.

International Committee for Information Technology Standards (2003) *Smart Card Biometric Interoperability Study Report*. INCITS Secretariat, Information Technology Industry Council, Washington DC: International Committee for Information Technology Standards. Online. Available: http://www.ncits.org/tc_home/m1htm/docs/m1030398.pdf (accessed 14 August 2007).

Information Technology Laboratory, NIST (2000) *Fingerprint Comparison Flash File,* February. Online. Available: http://www.itl.nist.gov/iad/894.03/fing/ fngcmps.html (accessed 13 August 2007).

Justice, Crime Prevention and Security (JCPS) Cluster briefing. (2007) 16 February. Online. Available: http://www.pmg.org.za/briefings/briefings.php? id=319 (accessed 30 May 2007).

Lloyd, T. (2000) 'Strange bedfellows, but they make a smart pair', *Financial Mail* 14 July.

National Institute of Standards and Technology (2006) Minutiae Interoperability Exchange Test 2004. Online. Available: http://fingerprint.nist.gov/minex04/ (accessed 7 August 2007).

NEC Corporation (2006) 'NEC UK shows how global biometric solutions could enhance UK Border Control', 18 October. Online. Available: http://www.prnewswire.co.uk/cgi/news/release?id=181837 (accessed 27 May 2007).

Lunsche, S. (1997) 'Arm wrestling to take the nation's fingerprints', *Sunday Times* 1 June.

Lunsche, S. (1998) 'IT companies scramble for lucrative ID tender', *Sunday Times* 15 February.

Marais, H. (2001) *South Africa – Limits to Change: the Political Economy of Transition*, London: Zed Books.

Net 1 UEPS Technologies, Inc (2006) Net1 UEPS Technologies, Inc Annual Report, 30 June.

O'Meara, D. (1996) *Forty lost years: the apartheid state and the politics of the National Party, 1948–1994*. Johannesburg: Ravan Press.

Peachey-Warner, G. (2003) 'Biometric standardisation: HANIS smart ID card project and ARP 054 standard', *Elekron Journal – South African Institute of Electrical Engineers* 20(4): 55–6.

The Reconstruction and Development Programme (1994) Online. Available: http://www.anc.org.za/rdp/rdpall.html (accessed 25 May 2007).

Sengoopta, C. (2003) *Imprint of the Raj: How Fingerprinting was Born in Colonial India*, London: Macmillan.

Sergeant, B. (2005) 'Moneyweb – Historical news: Daily news – South Africa's $1.5-bn champion', *Moneyweb*, 5 August. Online. Available: http://www.moneyweb.co.za/mw/view/mw/en/page62053?oid=39903&sn=Daily%20news%20Detail (accessed 12 April 2007).

South African Department of Home Affairs (2003) 10 March. Online. Available: http://www.home-affairs.gov.za/projects.asp (accessed 3 June 2007).

Stirling, Tony (1988) 'Black sash claims on black IDs repudiated', *The Citizen* 8 January.

Stones, Lesley (1997) 'Race on to supply state ID system', *Business Day* 9 October.

Unisys & South Africa's Department of Home Affairs (2004) Combating fraud with instant identification verification. Online. Available: http://www.unisys.com/services/clients/featured_case_studies/sa_department_home_affairs.htm (accessed 4 January 2004).

van den Heever, J. (2001) 'IT in Government: slow and steady wins the race', *Computer Week*, 30 July. Online. Available: http://homeaffairs.pwv.gov.za/ news.asp?id=2 (accessed 11 April 2007).

Warner, G. (2001) *Establishment of a national fingerprint biometric standard for government*. Online. Available: http://home-affairs.pwv.gov.za/documents/presentations/position%20paper.zip (accessed 11 April 2007).

Warner, G. (2007a) *Interview*.

Warner, G. (2007b). *Interview 2*.

Whitby, P. (2000) 'Research on new citizen card begins', *Business Day* 7 April.

Wright, B. (2002) 'eGovernment', *SA Computer Magazine* 18 February. Online. Available: http://www.sacm.co.za/Feature.asp?NewsID=4203&Item=4835&Title =e%2DGovernment (accessed 11 April 2007).